SECTION II—REMARKS

Applicants thank the Examiner for a thorough review, and respectfully request reconsideration of the above referenced patent application for the following reasons:

Examiner's Interview:

On October 21, 2008, Examiner Techane J. Gergiso spoke with Applicants' representative, Spencer K. Hunter, a law clerk working under the discretion of Gregory D. Caldwell, who is the undersigned attorney for Applicant.

The interview is discussed in more detail below, under the remarks pertaining to the rejection under 35 U.S.C. § 103.

Objection to claim 40

The Office Action objected to claim 40 due to informalities.

Applicants respectfully submit that the amendments to claims overcome the objection. Accordingly, Applicants respectfully request the Examiner to withdraw the objection to claim 40.

Claims 26-44 rejected under 35 U.S.C. § 103(a)

The Office Action rejected claims 26-44 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent Application Publication No. 2004/0006708 to Mukherjee et al. ("Mukherjee") in view of U.S. Patent Application Publication No. 2003/0041136 to Cheline et al. ("Cheline").

During Applicants' interview with the Examiner, the problem addressed by the present

invention was discussed in detail. In particular, Applicants explained that a network switching device or other packet forwarding device connected with a network may leave the network exposed to attack from computing devices, regardless of whether the computing devices are authorized access resources within the network. This is because a conventional network switch allows computing devices to connect with the network by default and initiate packet data that is transmitted into the network by the packet forwarder, without challenging the authenticity of the computing device or a user of the computing device.

Conventional network switches instead rely upon computer servers within the network to challenge the authenticity of a user, however, malicious network traffic may have already been introduced into the network before any such authentication process is begun. These concepts are discussed in Applicants' original specification, as follows:

> [**0004**] The difficulties associated with securing a network have existed ever since computer networks were first introduced. Over the years a variety of techniques have been employed to provide network security. **Generally most of these security techniques take place between network nodes** (a node is an end point for data transmissions, such as **a computer workstation, network server, CD-ROM jukebox, or some other such device**) and not between connection points (a connection point is an intermediate point in the network, such as a router, hub, or a switch). … .
>
> * * *
>
> [**0010**] For example, access lists were developed to combat cyber-attacks on the LAN …
>
> [**0011**] A major drawback to access lists, DoS, and SYN attack protections is that access to the network is machine- or hardware-based instead of user-based. **Therefore, an unauthorized user who has access to an authorized machine can still gain access to the network, completely bypassing the intended security protection**. Moreover, publicly accessed network resources, e.g. a web server not protected by a firewall, are **more susceptible since access to a public resource cannot usually be restricted to certain machines or IP addresses**. Finally, most of the security measures currently in place to defend

against such attacks are proprietary and therefore expensive to implement.

Applicants further discussed with the Examiner, the concept of a packet forwarding device that expressly "**blocks**" all IP traffic generated within a particular VLAN from accessing the network. While Applicants and the Examiner were unable to agree on specific language for a claim due to time constraints, the Examiner did express that a claim which explicitly incorporates such a concept, in addition to the other limitations previously presented, may be patentable over the prior art of record, subject of course to a detailed review and a new search.

In accordance with Applicants' discussion with the Examiner, independent claim 26, has been amended herein to recite in pertinent part:

> receiving a connection request from an **unauthorized computing device** at a first port of the packet forwarder …
> **blocking all data packets** received at the first port of the packet forwarder **from accessing the network**;
> issuing the unauthorized computing device a first [IP] … assigned to a first [VLAN] … operating within the packet forwarder and associated with the first port, wherein the first VLAN does not provide access to the network communicably interfaced with the packet forwarder via the second port, and wherein **the packet forwarder blocks the data packets in the first VLAN from reaching a permanent VLAN that provides access to the network**, permanent VLAN operating within the packet forwarder associated with the second port of the packet forwarder and not the first port of the packet forwarder …
> authorizing the computing device …
> forwarding the data packets … .

Applicants teach "**blocking all data packets**" in the specification as originally filed. For example, refer to Figure 4, element 170, and the corresponding teachings from the specification:

> [**0034**] FIG. 4 is a block diagram illustrating the ports 205 and 206 and their respective port statuses 207/208 in further detail … . As shown, each port may be in a different state depending on whether or not an authorized user has connected to the port and successfully completed the network login authorization (or depending on whether network login authorization has been

> activated for that port or for the VLAN of the host connected to that port). In the example illustrated in FIG. 4, port 205 has a port state 207 of unauthorized. **The unauthorized port state 207 of port 205 places the port 205 into a non-forwarding mode 170. Non-forwarding mode 170 causes the packet forwarder 160 to block packets to and from the port 205**. Conversely, the port state 208 of port 206 is authorized, which places the port 206 into a forwarding mode 180. Forwarding mode 180 causes the packet forwarder 160 to send and receive packets to and from the port 206 as it normally would.

Thus, Applicants teach in the specification, a packet forwarder capable of "blocking all data packets associated with the unauthorized computing device," as Applicants recite in claim 26.

The use of a first VLAN for "authorizing the computing device" before assigning the computing device into a "**permanent VLAN that provides access to the network**" is likewise taught in the specification, for example,

> [**0030**]… In the campus environment, the port through which the user connects **is not assigned to a permanent VLAN** (i.e. layer-2 domain) until the user is authorized through the network login authorization. … .
>
> [**0031**] … In both the campus and network provider environments, prior to authorization through network login authorization, the user **obtains a temporary layer-3 address in order to gain access to the authenticator discovery controller** 190, the network login controller 110, and user interface 120 on packet-forwarding device 200. … .
>
> * * *
>
> [**0042**] FIG. 6 is a flow diagram illustrating certain aspects of a method to be performed by a computer executing authenticator discovery according to one embodiment of the invention. … In one embodiment, the **user device may need to obtain a temporary IP address** from an IP address server 130 accessible to packet forwarding device 200.

Mukherjee and Cheline fail to disclose the limitations of claims 26-44:

Applicants respectfully submit that Mukherjee does not disclose a packet forwarding device capable of, "**blocking all data packets** associated with the unauthorized computing

device from accessing the network," as Applicants recite in claim 26.

Mukherjee describes a mechanism for "providing peer-to-peer virtual private network (P2P-VPN) services over a network" including, initiating a "virtual private host (VPH)" that "communicates with each user device via a respective tunnel throughout the network, **thereby enabling secure communications between the user devices**." Refer to the Abstract of Mukherjee.

Mukherjee is silent, however, with regard to a packet forwarder that "**block[s] all data packets**," from an unauthorized computing device, thus preventing the kinds of attacks that are possible when an unauthorized device is permitted to transmit packets into a network. Rather than describing a mechanism for affirmatively "**blocking all data packets**," as claimed by Applicants, Mukherjee instead describes the process of, "**enabling secure communications**," which is precisely what Applicants' claimed method prevents, until such time that the "computing device" has been authorized to communicate on the network.

Mukherjee discloses a network environment in which the "computing device," such as a client, is already actively communicating on the network. The P2P-VPN services of Mukherjee simply enable "secure communications." Mukherjee does not, however, prevent communications (e.g., "data packets") from the computing device from entering into the network by "**blocking all data packets**," as Applicants recite in claim 26.

Cheline does not cure the deficiencies of Mukherjee as it too fails to disclose, "blocking all data packets associated with the unauthorized computing device," as Applicants recite in claim 26.

Because Mukherjee and Cheline, whether considered alone or in combination, fail to disclose at least one limitation as Applicants recite in independent claim 26, Applicants

respectfully submit that claim 26 is patentable over the references and in condition for allowance. Applicants further submit that independent claims 35 and 40, as well as those claims depending on independent claims 26, 35, and 40, are patentable over the references and in condition for allowance.

Applicants solve different problem than the Mukherjee and Cheline references:

Applicants teach in the original specification that networks, especially public networks which are accessible to a dynamic group of users, are especially susceptible to attack because an unauthorized machine may initiate data packets which are transmitted into the network by a conventional packet forwarder. To address such a problem, Applicants teach and claim a method for "**blocking all data packets** associated with the unauthorized computing device from accessing the network," as Applicants recite in claim 26.

Conversely, the Mukherjee and Cheline address problems associated with Virtual Private Networks (VPNs), and specifically disclose a mechanism by which VPN services may be provided by a service provider entity, otherwise unassociated with a network that is being accessed by a service subscriber. Mukherjee and Cheline discuss at some length, the necessary hardware and security components that are necessary to effectuate such a system.

Although Mukherjee and Cheline are related to network technology in general, they simply do not contemplate, nor do they address the specific problem described and solved by Applicants. Because Mukherjee and Cheline address a different problem than that of Applicants, the references do not overlap in any meaningful way, so as to provide a logical and plain language interpretation that would yield a compelling rejection of non-patentability.

Conclusion to 35 U.S.C. § 103 discussion:

In accordance with the preceding remarks, Applicants respectfully request that the Examiner withdraw the rejection to claims 26-44.

New claim 45:

Applicants respectfully submit that new claim 45 does not add new subject matter as it finds support in the specification, claims, and/or figures as originally presented. Accordingly, Applicants respectfully request the Examiner to allow new claim 45 as presented herein.

CONCLUSION

Given the above amendments and accompanying remarks, all claims pending in the application are in condition for allowance. If the undersigned attorney has overlooked subject matter in any of the cited references that is relevant to allowance of the claims, the Examiner is requested to specifically point out where such subject matter may be found. Further, if there are any informalities or questions that can be addressed via telephone, the Examiner is encouraged to contact the undersigned attorney at (503) 439-8778.

Charge Deposit Account

Please charge our Deposit Account No. 02-2666 for any additional fee(s) that may be due in this matter, and please credit the same deposit account for any overpayment.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

/Gregory D. Caldwell/

Date: November 24, 2008

Gregory D. Caldwell
Registration No. 39,926
Attorney for Applicants

Blakely, Sokoloff, Taylor & Zafman LLP
1279 Oakmead Parkway
Sunnyvale, CA 94085-4040
Telephone: (503) 439-8778
Facsimile: (503) 439-6073